Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Parkmobile, LLC (the Organization)
Decision number (file number)	P2022-ND-030 (File #022840)
Date notice received by OIPC	August 11, 2021
Date Organization last provided information	August 11, 2021
Date of decision	May 2, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is based in Atlanta, Georgia, USA and is an "organization" as defined in section 1(1)(i) of PIPA. The Organization provides electronic parking services.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • phone number, • mailing address (a small percentage of individuals), • license plate number, and • vehicle nickname (if provided). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about March 8, 2021, the Organization became aware of a cybersecurity incident. The incident is linked to a vulnerability in a third-party software.

	• On March 15, 2021, the breach was discovered when the Organization received an email from the unauthorized person who attacked the network. • The vulnerability allowed the unauthorized person access to a database table.
Affected individuals	The incident affected 3442 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Eliminated the vulnerability in the third party software. • Launched an investigation with the assistance of a cybersecurity firm. • Notified the Federal Bureau of Investigation. • Added a second penetration-testing vendor. • Suggested users change their passwords and use unique passwords for different online accounts. • Continues to maintain security and monitor its systems.
Steps taken to notify individuals of the incident	The Organization notified affected individuals by email and in-application notification on April 16, 2021.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported, *Our assessment concluded that there is not a real risk of significant harm. However, based on recent rulings from [sic] Office of the Information and Privacy Commissioner of Alberta, a possible harm to indiviuals [sic] could be an increase in email phishing campaigns.* In my view, a reasonable person would consider the contact information and email address could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported, *Our assessment concluded that there is not a real risk of significant of harm to the impacted individuals. However, in an effort to be transparent and in light of recent rulings from [sic] Office of the Information and Privacy Commissioner of Alberta, this report is being submitted.* *The personal information accessed by the unauthorized person is basic account information that an ordinary person does not keep private. This is information that could be obtained via an internet search. Our research shows that the personal*

	information involved can be obtained by any member of the public from mulitple [sic] search providers for less than USD$20. *Most importantly, the personal information involved does not contain any sensitive or financial information that could readily lead to bodily harm; embarassment [sic]; damage to reputation; loss of employment; financial loss; identity theft; fraud; negative effects on a credit record; damage to or loss of property; or blackmail or exortion[sic]. ParkMobile provides electronic parking services and does not collect sensitive information in its ordinary course of business that would readily lead to the aforementioned harms. As indicated in the notice individuals received, ParkMobile does not collect social security numbers, driver's license numbers, or dates of birth. While ParkMobile does collect payment card information, that information is encrypted and more importantly, is not at issue as a part of the security incident.* *Recent rulings from the Office of the Information and Privacy Commissioner of Alberta have indicated that risks of email phishing constitute a "real risk of significant harm." It is our opinion that this instance is different and does not rise to the level of a real risk of significant harm. Specifically, because the services ParkMobile provides are simply parking services and not something more susceptible to email phishing campaigns such as banking or healthcare. A ParkMobile user would know that something was awry if a phishing email asked for information such as banking details, social security number, date of birth, etc. because none of those items are needed to complete a parking services transaction with ParkMobile.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization reported, "...the services ParkMobile provides are simply parking services and not something more susceptible to email phishing campaigns such as banking or healthcare..." I do not find this to be reassuring. The Organization can only speculate as to the motives of the unknown third party. The Organization was able to eliminate the vulnerability in the third party software; however, personal information was acquired without authorization during the incident. The attacks appear to have been ongoing for approximately 9 days before the Organization discovered the threat.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. In my view, a reasonable person would consider the contact information and email address could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization reported, "...the services ParkMobile provides are simply parking services and not something more susceptible to email phishing campaigns such as banking or healthcare..." I do not find this to be reassuring. The Organization can only speculate as to the motives of the unknown third party. The Organization was able to eliminate the vulnerability in the third party software; however, personal information was acquired without authorization during the incident. The attacks appear to have been ongoing for approximately 9 days before the Organization discovered the threat. I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by email and in-application notification on April 16, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner